1. A method for securing an accessible computer system, the method comprising:

receiving a data packet that includes a payload portion and an attribute portion and is communicated between at least one access requestor and at least one access provider;

monitoring at least the payload portion of the data packet received by scanning the payload portion for at least one predetermined pattern; and

controlling access by the access requestor to the access provider when the payload portion is determined to include at least one predetermined pattern.

2. The method as in claim 1 wherein:

receiving the data packet includes receiving more than one data packet; and

monitoring the data packet includes counting the number of data packets having payload portions that include the predetermined pattern.

3. The method as in claim 1 wherein monitoring the data packet includes scanning the payload portion while handling the data packet with a switch.

4. The method as in claim 3 wherein:

receiving the data packet includes receiving more than one data packet; and

monitoring the data packet includes monitoring only at least one data packet that is distinguished.

5. The method as in claim 1 wherein:

receiving the data packet includes receiving more than one data packet,

securing the accessible computer system further comprises distinguishing at least one of the data packets from among the data packets received for additional processing, and

monitoring the payload portion includes monitoring the payload portion of the at least one data packet distinguished.

6. The method as in claim 5 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

7. The method as in claim 1 wherein:

receiving the data packet includes receiving more than one data packet; and

monitoring the data packet includes monitoring all of the data packets received.

8. The method as in claim 1 wherein the access requestor is a client and the access provider is a host.

9. The method as in claim 8 wherein the data packet is monitored when communicated from the client to the host.

10. The method as in claim 8 wherein the data packet is monitored when communicated from the host to the client.

11. The method as in claim 8 wherein the predetermined pattern includes a login failure message communicated from the host to the client.

12. The method as in claim 1 wherein the data packet includes a token-based protocol packet.

13. The method as in claim 1 wherein the data packet includes a TCP packet.

14. The method as in claim 1 wherein the data packet includes a PPP packet.

15. The method as in claim 1 wherein controlling access includes denying access by the access requestor to the access provider.

16. The method as in claim 1 wherein controlling access includes affecting bandwidth for communications between the access requestor and the access provider.

17. The method as in claim 1 wherein controlling access includes rerouting the access requestor.

18. The method as in claim 2 wherein:

receiving the data packet includes receiving more than one data packet; and

controlling access by the access requestor to the access provider includes denying access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number.

19. The method as in claim 18 wherein controlling access by the access requestor to the access provider includes denying access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

20. A system for securing an accessible computer system, comprising:

a receiving component that is structured and arranged to receive a data packet that includes a payload portion and an attribute portion and is communicated between at least one access requestor and at least one access provider;

a monitoring component that is structured and arranged to monitor at least the payload portion of the data packet received and includes a scanning component that is structured and arranged to scan the payload portion for at least one predetermined pattern; and

an access controlling component that is structured and arranged to control access by the access requestor to the access provider when the payload portion is determined to include at least one predetermined pattern.

21. The system of claim 20 wherein:

the receiving component is structured and arranged to receive more than one data packet; and

the monitoring component further includes a counting component that is structured and arranged to count the number of data packets having payload portions that include the predetermined pattern.

22. The system of claim 20 wherein the monitoring component includes a scanning component that is structured and arranged to scan the payload portion while handling the data packet with a switch.

23. The system of claim 22 wherein:

the receiving component is structured and arranged to receive more than one data packet; and

the monitoring component is structured and arranged to monitor only at least one data packet that is distinguished.

24. The system of claim 20 wherein:

the receiving component is structured and arranged to receive more than one data packet,

the system further comprises a distinguishing component that is structured and arranged to distinguish at least one of the data packets from among the data packets received for additional processing, and

the monitoring component is structured and arranged to monitor the payload portion of the at least one data packet distinguished.

25. The system of claim 24 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

26. The system of claim 20 wherein:

the receiving component is structured and arranged to receive more than one data packet; and

the monitoring component is structured and arranged to monitor all of the data packets received.

27. The system of claim 20 wherein the access requestor is a client and the access provider is a host.

28. The system of claim 27 wherein the data packet is monitored when communicated from the client to the host.

29. The system of claim 27 wherein the data packet is monitored when communicated from the host to the client.

30. The system of claim 27 wherein the predetermined pattern includes a login failure message communicated from the host to the client.

31. The system of claim 20 wherein the data packet includes a token-based protocol packet.

32. The system of claim 20 wherein the data packet includes a TCP packet.

33. The system of claim 20 wherein the data packet includes a PPP packet.

34. The method as in claim 20 wherein the access controlling component is structured and arranged to deny access by the access requestor to the access provider.

35. The system of claim 20 wherein the access controlling component is structured and arranged to affect bandwidth for communications between the access requestor and the access provider.

36. The system of claim 20 wherein the access controlling component is structured and arranged to reroute the access requestor.

37. The system of claim 21 wherein:

the receiving component is structured and arranged to receive more than one data packet; and

the access controlling component is structured and arranged to deny access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number.

38. The system of claim 37 wherein the access controlling component is structured and arranged to deny access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.

39. A computer program stored on a computer readable medium or a propagated signal for securing an accessible computer system, comprising:

a receiving code segment that causes the computer to receive a data packet that includes a payload portion and an attribute portion and is communicated between at least one access requestor and at least one access provider;

a monitoring code segment that causes the computer to monitor at least the payload portion of the data packet received and includes a scanning code segment that causes the computer to scan the payload portion for at least one predetermined pattern; and

an access controlling code segment that causes the computer to control access by the access requestor to the access provider when the payload portion is determined to include at least one predetermined pattern.

40. The computer program of claim 39 wherein:

the receiving code segment causes the computer to receive more than one data packet; and

the monitoring code segment further includes a counting code segment that causes the computer to count the number of data packets having payload portions that include the predetermined pattern.

41. The computer program of claim 39 wherein the monitoring code segment includes a scanning code segment that causes the computer to scan the payload portion while handling the data packet with a switch.

42. The computer program of claim 41 wherein:

the receiving code segment causes the computer to receive more than one data packet; and

the monitoring code segment causes the computer to monitor only at least one data packet that is distinguished.

43. The computer program of claim 39 wherein:

the receiving code segment causes the computer to receive more than one data packet,

the computer program further comprises a distinguishing code segment that causes the computer to distinguish at least one of the data packets from among the data packets received for additional processing, and

the monitoring code segment causes the computer to monitor the payload portion of the at least one data packet distinguished.

44. The computer program of claim 43 wherein the at least one data packet is distinguished based on an Internet address associated with the data packet.

45. The computer program of claim 39 wherein:

the receiving code segment causes the computer to receive more than one data packet; and

the monitoring code segment causes the computer to monitor all of the data packets received.

46. The computer program of claim 39 wherein the access requestor is a client and the access provider is a host.

47. The computer program of claim 46 wherein the data packet is monitored when communicated from the client to the host.

48. The computer program of claim 46 wherein the data packet is monitored when communicated from the host to the client.

49. The computer program of claim 46 wherein the predetermined pattern includes a login failure message communicated from the host to the client.

50. The computer program of claim 39 wherein the data packet includes a token-based protocol packet.

51. The computer program of claim 39 wherein the data packet includes a TCP packet.

52. The computer program of claim 39 wherein the data packet includes a PPP packet.

53. The computer program of claim 39 wherein the access controlling code segment causes the computer to deny access by the access requestor to the access provider.

54. The computer program of claim 39 wherein the access controlling code segment causes the computer to affect bandwidth for communications between the access requestor and the access provider.

55. The computer program of claim 39 wherein the access controlling code segment causes the computer to reroute the access requestor.

56. The computer program of claim 40 wherein:

the receiving code segment causes the computer to receive more than one data packet; and

the access controlling code segment causes the computer to deny access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number.

57. The computer program of claim 56 wherein the access controlling code segment causes the computer to deny access by the access requestor to the access provider when a number of payload portions that include the predetermined pattern exceed a configurable threshold number during a configurable period of time.